WHAT IS CLAIMED IS:

1. A public-key cryptographic scheme comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $\qquad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2},\ d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}},\ d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}},\ h = {g_1}^{z},$
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

where M is a plaintext space;

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$ for a plaintext m ($m \in M$), calculating:

$$u_1 = {g_1}^{r}, \quad u_2 = {g_2}^{r}, \quad e = \pi(\alpha_1, \alpha_2, m) h^{r}, \quad v = {g_1}^{\alpha_1} c^{r} {d_1}^{\alpha r} {d_2}^{mr}$$

where $\alpha = \alpha_1 \; || \; \alpha_2$, and transmitting ($u_1$, u_2, e, v) as a ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using

the secret key, α'_1, α'_2, m' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, $m' \in M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e/{u_1}^z$$

and if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1+\alpha' y_{11}+m' y_{21}} {u_2}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 \| \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

2. A public-key cryptographic scheme comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = {g_1}^{x_1} {g_2}^{x_2} \bmod p$, $d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}} \bmod p$, $d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}} \bmod p$, $h = {g_1}^z \bmod p$,
- k_1, k_2, k_3 : positive constant ($10^{k_1+k_2} < q$, $10^{k_3} < q$, $10^{k_1+k_2+k_3} < p$)

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \| \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$ where $|x|$ is the number of digits of x), calculating:

$$\tilde{m} = \alpha \| K$$

selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad e = \widetilde{\mathrm{m}}\ h^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{mr} \bmod p$$

and transmitting (u_1, u_2, e, v) as a ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|m'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = e/u_1{}^z \bmod p$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_{11} + m' y_{21}} u_2{}^{x_2 + \alpha' y_{12} + m' y_{22}} \equiv v \pmod{p}$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

3. A public-key cryptographic scheme according to claim 1, wherein the public-key is generated by a receiver and is made public.

4. A public-key cryptographic scheme according to claim 1, wherein in said ciphertext transmission step, the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$ and $r \in Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad h^r, \quad g_1{}^{\alpha_1} c^r d_1{}^{\alpha r}$$

5. A public-key cryptographic scheme according to claim 2, wherein in said ciphertext transmission

step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \in Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = {g_1}^r \bmod p, \quad u_2 = {g_2}^r \bmod p, \quad h^r \bmod p, \quad {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} \bmod p$$

6. A cryptographic communication method comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2}$, $d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}}$, $d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}}$, $h = {g_1}^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

where M is a key space;

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$ for key data K ($K \in M$), calculating:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad e = \pi(\alpha_1, \alpha_2, K) h^r, \quad v = {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} {d_2}^{Kr}$$

where $\alpha = \alpha_1 \mid\mid \alpha_2$, generating a ciphertext C of transmission data m by:

$$C = E_K(m)$$

by using a (symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, $K' \in M$) which satisfy:

$$\pi(\alpha'_1 || \alpha'_2 || K') = e / {u_1}^z$$

and if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_{11} + K' y_{21}} {u_2}^{x_2 + \alpha' y_{12} + K' y_{22}} = v$$

where $\alpha' = \alpha'_1 \mid\mid \alpha'_2$

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

7. A cryptographic communication method according to claim 6, wherein the ciphertext C is generated by:

$$C = E_K(f(\alpha_1, \alpha_2) || m)$$

by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} = v,$$
$$f(\alpha'_1, \alpha'_2) = [D_{K'}(C)]^k$$

where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:

$$m = [D_{K'}(C)]^{-k}$$

where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed.

8. A cryptographic communication method comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p,\ d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p,\ d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p,\ h = g_1^{z} \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- E : symmetric encipher function

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for key data K ($|K| = k_3$ where $|x|$ is the number

of digits of x), calculating:

$$\tilde{\mathrm{m}} = \alpha || K$$

selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad e = \tilde{\mathrm{m}}\, h^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{Kr} \bmod p$$

and generating a ciphertext C of transmission data by:

$$C = E_K(m)$$

by using a (symmetric) cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|K'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || K' = e / u_1{}^z \bmod p$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_{11} + K' y_{21}} u_2{}^{x_2 + \alpha' y_{12} + K' y_{22}} \equiv v \pmod{p}$$

where $\alpha' = \alpha'_1 \,||\, \alpha'_2$,

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

9. A cryptographic communication method according to claim 8, wherein the ciphertext C is generated by:

$$C = E_K(f(\alpha_1, \alpha_2) \| m)$$

by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod{p},$$
$$f(\alpha'_1, \alpha'_2) = [D_{K'}(C)]^k$$

where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:

$$m = [D_{K'}(C)]^{-k}$$

where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed.

10. A cryptographic communication method according to claim 6, wherein the public-key is generated by a receiver and is made public.

11. A cryptographic communication method according to claim 6, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \in X_1$, $\alpha_2 \in X_2$) and $r \in Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad h^r, \quad g_1^{\alpha_1} c^r d_1^{\alpha r}$$

12. A cryptographic communication method according to claim 6, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) and $r \in Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = {g_1}^r \bmod p, \quad u_2 = {g_2}^r \bmod p, \quad h^r \bmod p, \quad {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} \bmod p$$

13. A cryptographic communication method comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $\quad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2},\ d = {g_1}^{y_1} {g_2}^{y_2},\ h = {g_1}^z,$
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping (Dom(E) is the domain of the function E)
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- H : hash function
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

a ciphertext generation and transmission step

of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$, calculating:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r}, \quad K = H(h^r)$$

where $\alpha = \alpha_1 \,||\, \alpha_2$, generating a ciphertext C of transmission data m by

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

by using a (symmetric) cryptographic function E; and transmitting (u_1, u_2, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating:

$$K' = H(u_1{}^z)$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 (where $\alpha'_1 \in X_1$ $\alpha'_2 \in X_2$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_1} u_2{}^{x_2 + \alpha' y_2} = v,$$

where $\alpha' = \alpha'_1 \,||\, \alpha'_2$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

14. A cryptographic communication method comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = {g_1}^{x_1} {g_2}^{x_2} \bmod p,\ d = {g_1}^{y_1} {g_2}^{y_2} \bmod p,\ h = {g_1}^{z} \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- H : hash function
- E : symmetric encipher function (the domain of E is all positive integers)

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \mid\mid \alpha_2$ $(|\alpha_1| = k_1,\ |\alpha_2| = k_2$, where $(|x|$ is the number of digits of $x)$, selecting a random number $r \in Zq$, calculating:

$$u_1 = {g_1}^{r} \bmod p, \quad u_2 = {g_2}^{r} \bmod p, \quad v = {g_1}^{\alpha_1} c^{r} d^{\alpha r} \bmod p, \quad K = H(h^{r} \bmod p)$$

transmitting the ciphertext (u_1, u_2, v, C); generating a ciphertext C of transmission data m by:

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

by using a (symmetric) cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext;

a ciphertext reception and decipher step of calculating:

$$K' = H({u_1}^{z} \bmod p)$$

by using the secret key, calculating from the received

ciphertext, α'_1, α'_2 ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$) which satisfy:

$$\alpha'_1||\alpha'_2||m' = D_{K'}(C)$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1}u_1{}^{x_1+\alpha' y_1}u_2{}^{x_2+\alpha' y_2} \equiv v \pmod p$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

15. A cryptographic communication method according to claim 13, wherein the public-key is generated by a receiver and is made public.

16. A cryptographic communication method according to claim 13, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \in X_1$, $\alpha_2 \in X_2$) and $r \in Zq$ are selected beforehand and the u_1, u_2, e and v are calculated and stored beforehand.

17. A cryptographic communication method according to claim 14, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \in Zq$ are selected beforehand and the u_1, u_2, e and v are calculated and stored beforehand.

18. A cryptographic communication method comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and a public-key:

- G : finite (multiplicative) group
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1}{g_2}^{x_2},\ d = {g_1}^{y_1}{g_2}^{y_2},$
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping (Dom(E) is the domain of the function E)
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

where M is a plaintext space;

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$, calculating:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad v = {g_1}^{\alpha_1} c^r d^{\alpha r}$$

where $\alpha = \alpha_1 \ || \ \alpha_2$, generating a ciphertext C of transmission data m by:

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

by using an (asymmetric) cryptographic function E_{pk}, and transmitting (u_1, u_2, e, v) as the ciphertext; and

a ciphertext reception and decipher step of

calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \in X_1$, $\alpha'_2 \in X_2$, $m' \in M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{sk}(e)$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

19. A cryptographic communication method comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p,\ d = g_1{}^{y_1} g_2{}^{y_2} \bmod p,$
- k_1, k_2 : positive constant $(10^{k_1+k_2} < q)$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function (the domain is all positive integers)

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x), selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r} \bmod p$$

generating a ciphertext C of transmission data m (positive integer) by:

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, m' is a positive integer) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{sk}(e)$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_1} u_2{}^{x_2 + \alpha' y_2} \equiv v \pmod{p},$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

20. A cryptographic communication method according to claim 18, wherein the public-key is

generated by a receiver and is made public.

21. A cryptographic communication method according to claim 18, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \in X_1$, $\alpha_2 \in X_2$) and $r \in Zq$ are selected beforehand and the u_1, u_2 and v are calculated and stored beforehand.

22. A cryptographic communication method according to claim 19, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \in Zq$ are selected beforehand and the u_1, u_2 and v are calculated and stored beforehand.